REMARKS

The Final Office Action mailed March 19, 2010, considered and rejected claims 1-20. Claims 4, 14-16 and 20 were rejected under 35 U.S.C. 101 because the claimed invention was directed to non-statutory subject matter. Claims 1-20 were rejected under 35 U.S.C. 103(a) as being unpatentable over White et al. ("Anatomy of a Commercial-Grade Immune System") hereinafter *White* in view of Schultz et al. (US 2003/0065926) hereinafter *Schultz* in further view of Obrecht et al. (US 2004/0054917) hereinafter *Obrecht*.[1]

101 Rejections

The paragraph added to the specification in the last response has been amended in this response to clarify the distinction between storage media and communication media. These amendments do not add new matter because they only provide terms to be used to sub-divide computer-readable media into statutory and non-statutory categories. In particular, storage media is defined as including all computer-readable media except signals, whereas communication media includes signals. Inasmuch as claims 4 and 16 recite storage media rather than communication media, it cannot be argued that they encompass signals.

Prior Art Rejections

By this response, each of the independent claims has been amended to clarify that the invention is directed to embodiments which record only interesting function calls that a code module makes during execution. This is described primarily on page 7 of the specification. In particular, it states that "interesting behaviors are those which a user or implementer of the malware detection system has identified as interesting, potentially associated with malware, and are used to compare the behaviors of the code module against known malware behaviors." As an example, the table of page 7 lists many different function calls that could be considered as "interesting function calls." Applicant submits that this table provides support for the limitation that the interesting behaviors described in the specification are in fact function calls. Further, to support the limitation that the function calls are a subset of all function calls that a code module makes, the specification states that a user must specify which interesting behaviors are to be recorded. This would not be necessary if all behaviors, or function calls, were recorded.

[1] Although the prior art status of the cited art is not being challenged at this time, Applicant reserves the right to challenge the prior art status of the cited art at any appropriate time, should it arise. Accordingly, any arguments and amendments made herein should not be construed as acquiescing to any prior art status of the cited art.

Once the interesting function calls have been recorded, they form the behavior signature for the code module. This behavior signature is compared to the behavior signature for known malware to determine whether the code module is malware. This comparison involves comparing the interesting function calls made by the code module to those that are known to be made by known malware.

The distinction of recording only interesting function calls did not appear previously in the claims. As a result, none of the references are relevant to this newly added feature. In particular, White only tangentially relates to heuristic, or behavior based, detection. Page 11, for example, states that viruses can be detected by simulated their execution and recording their behavior, but no further details are provided about how this is done.

Schultz, on the other hand, is related to virus detection in binaries that is performed without executing the binaries. *See* ¶ 42. Because the binaries are not executed, Schultz is not relevant to behavioral based detection because it requires execution to detect which function calls are made.

Finally, Obrecht mentions that the behavior of a potential malware program can be monitored (*see* ¶ 20), but nothing is stated about recording only specified "interesting function calls," as required by the claims.

In summary, none of the cited references disclose or suggest that only interesting function calls are recorded during emulation of a potential malware, or that these interesting function calls can be used to determine whether the potential malware is in fact malware by comparing the interesting function calls to those made by known malware. As such, these references in combination fail to teach or suggest:

> at least one dynamic behavior evaluation module, wherein each dynamic behavior evaluation module provides a virtual environment for executing a code module of a particular type, and *wherein each dynamic behavior evaluation module records interesting function calls that the code module makes as it is executed, wherein the interesting function calls are specified by a user and comprise a subset of all function calls that the code module makes, wherein only the interesting function calls, but not all function calls, that the code module makes during execution in the dynamic behavior evaluation module are recorded into a behavior signature corresponding to the code module*;
>
> a management module, wherein the management module obtains the code module, and wherein the management module evaluates the code module to determine the code module's type, and wherein the management module selects a dynamic behavior evaluation module to execute the code module according to the

code module's type;

a malware behavior signature store storing at least one known malware behavior signature of a known malware, *wherein each of the at least one known malware behavior signature is comprised of only interesting function calls as specified by the user*;

a behavior signature comparison module that obtains the behavior signature of the code module and compares the behavior signature of the code module to the known malware behavior signatures in the malware behavior signature store *to determine whether the interesting function calls recorded in the behavior signature of the code module match the interesting function calls in any of the known malware behavior signatures*; and

wherein the malware detection system is configured to report whether the code module is a known malware based at least in part on the degree that *the interesting function calls recorded in the behavior signature of the code module match the interesting function calls in a behavior signature of the known malware*;

as claimed in claim 1, or as similarly claimed in the remaining independent claims. Applicant, therefore, respectfully requests that the rejections be withdrawn.

In view of the foregoing, Applicant respectfully submits that the other rejections to the claims are now moot and do not, therefore, need to be addressed individually at this time. It will be appreciated, however, that this should not be construed as Applicant acquiescing to any of the purported teachings or assertions made in the last action regarding the cited art or the pending application, including any official notice. Instead, Applicant reserves the right to challenge any of the purported teachings or assertions made in the last action at any appropriate time in the future, should the need arise. Furthermore, to the extent that the Examiner has relied on any Official Notice, explicitly or implicitly, Applicant specifically requests that the Examiner provide references supporting the teachings officially noticed, as well as the required motivation or suggestion to combine the relied upon notice with the other art of record.

In the event that the Examiner finds remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney at (801) 533-9800.

The Commissioner is hereby authorized to charge payment of any of the following fees that may be applicable to this communication, or credit any overpayment, to Deposit Account No. 23-3178: (1) any filing fees required under 37 CFR § 1.16; and/or (2) any patent application and reexamination processing fees under 37 CFR § 1.17; and/or (3) any post issuance fees under

37 CFR § 1.20. In addition, if any additional extension of time is required, which has not otherwise been requested, please consider this a petition therefore and charge any additional fees that may be required to Deposit Account No. 23-3178.

Dated this 20th day of September, 2010.

Respectfully submitted,

/BRIAN D. TUCKER/

RICK D. NYDEGGER
Registration No. 28,651
BRIAN D. TUCKER
Registration No. 61,550
Attorneys for Applicant
Customer No. 47973

RDN:BDT
2809699_1